Des hackers combinent Elasticsearch et Cloud pour lancer des attaques DDoS

Des pirates ont profité d'une vulnérabilité dans le logiciel Open Source Elasticsearch pour mener des attaques en déni de service depuis le cloud d'Amazon.

Le 29 juillet 2014 par Jacques Cheminat 0

Tweeter

Les chercheurs de Kaspersky ont découvert une faille de sécurité dans le logiciel Open Source **Elasticsearch**, un moteur de recherche qui repose sur Lucene (pour indexer et chercher du texte). Il est très utilisé par les entreprises. Cette faille permet l'injection d'un malware capable de générer des attaques en déni de service.

« **Backdoor.Linux.Ganiw** » **a été trouvé en juin dernier** par les spécialistes de Kaspersky et utilise la technologie d'amplification de DNS qui augmente considérablement le trafic des attaques DDoS. En envoyant des requêtes qui s'apparentent au domaine de la victime, l'amplification de DNS accroît le volume des attaques par 10 voire plus et elles sont très difficiles à contrer. La faille, identifiée sous l'appellation CVE-2014-3120, touche les versions 1.1.x d'Elasticsearch, mais les scripts dynamiques impactés ont été désactivés dans les dernières versions 1.2 et 1.3 livrées récemment.

Un proof of concept sur les Cloud public

Pour augmenter encore un peu plus ces attaques, **Kurt Baumgartner**, expert chez Kasperky Lab a expliqué **dans un blog** qu'elles sont menées depuis des services Cloud comme EC2 d'Amazon, mais également sur des offres concurrentes. Les cybercriminels ont réussi à travailler sur une variante de la faille dans Elasticsearch qui donne la possibilité d'exécuter des commandes Linux à distance via une fenêtre bash shell. Le backdoor Gani peut ainsi installer plusieurs autres scripts malveillants sur les PC compromis comme Backdoor.Perl.RShell.c et Backdoor.Linux.Mayday.g. C'est ce dernier qui a été repéré sur des instances EC2 par les spécialistes de Kasperky Lab.

Kurt Baumgartner indique que « *le flux est assez important pour qu'Amazon informe aujourd'hui ses clients de ce problème. Car* ***certains utilisateurs impactés vont se retrouver avec une facture salée*** *pour usage excessif de ressources* ». L'expert constate que les attaques concernent « *une grande banque régionale américaine, un grand fabricant d'électronique et un fournisseur de service au Japon* ». Reste qu'il se veut rassurant en expliquant que les attaques depuis des instances EC2 n'envoient que du trafic UDP et n'utilisent pas la technologie d'amplification de DNS. Cela signifie que les pirates sont encore en phase de test pour mener leurs attaques et qu'ils peaufinent leur méthode.

A lire aussi :

Une accalmie toute relative pour les attaques DDoS début 2014
DDoS : les entreprises françaises attaquées... mais insouciantes

Restez connectés, inscrivez-vous gratuitement à notre newsletter ! >>

Auteur: Jacques Cheminat

Rédacteur en chef
Lire mes autres articles

ZONES PARTENAIRES

QUIZ

Les derniers quiz :

- Tout sur le Bluetooth
- Êtes-vous un expert des langages de programmation ?
- 10 questions sur les noms des systèmes d'exploitation
- Les applications Android business
- Tout sur l'Ethernet

Voir tous les quiz disponibles

BLOG

Les acheteurs aussi ont droit à leur solution de mobilité

Contenu sponsorisé par Ariba / SAP

La vérification des tarifs fournisseurs : une source majeure d'économies

Contenu sponsorisé par Ariba / SAP

En finir avec le flou autour des dépenses en prestations

Contenu sponsorisé par Ariba / SAP

EMPLOI SUR SILICON.FR

Formez-vous au métier :Chef de projet digital

Mon article vous a plu ?
Restez-connectés en vous inscrivant à nos newsletters

Suivez-moi
Google + Twitter Facebook Linkedin

Autres articles sur ce sujet

Open World Forum – Red Hat : « L'open

Pour ses 10 ans, le projet Eclipse

Red Hat libère le code de son PaaS

La solution décisionnelle

CLOUD : ACCÉLÉRATEUR DE BUSINESS

Tout savoir sur les atouts Cloud pour la DSI !
Accédez au site Cloud : Accélérateur de Business et découvrez les dossiers et articles dédiés au Cloud, visualisez les vidéos interviews et témoignages clients et téléchargez gratuitement les études et livres blancs.

LIVRES BLANCS ASSOCIÉS

Pour bien commencer avec le Cloud
24.07.2014, Sage

Nouvelles exigences pour la sécurité, la conformité et l'audit dans le Cloud
15.07.2014, Qualys

Une sécurité basée sur la confiance et non pas sur la peur
15.07.2014, Qualys

Sécurité et virtualisation - Conseils pratiques pour vous aider à protéger vos systèmes et données sensibles
20.06.2014, Kaspersky

Voir tous nos livres blancs ...

AVAST! ANTIVIRUS

Près de 200 millions de personnes font confiance à avast! pour protéger leurs appareils - plus que tout autre antivirus Et il devient encore meilleur. Téléchargez- le maintenant !

« Précédent Suivant »

Tags : Amazon EC2, Cloud, DDoS, Kaspersky, open source, Sécurité.

DERNIERS COMMENTAIRES

0 replies to *Des hackers combinent Elasticsearch et Cloud pour lancer des attaques DDoS*

Laisser un commentaire

Les champs obligatoires sont indiqués avec *,
Votre adresse de messagerie ne sera pas publiée.

Nom*

E-Mail*

Site web

Commentaire

chez **IFOCOP**, Rungis

Ingénieur / Ingénieure système réseau informatique
chez **Source Pôle Emploi**, Angers

HOTLINER NIVEAU 2 (H/F)
chez **Adecco**, Cergy

Chef de projet web – Animation commerciale H/F
chez **WEBPOPULATION**, Paris

Formation Vendeur téléphonie mobile (H/F)
chez **CFA Ducretet**, Ile de France

Plus d'emplois ...

Publier une offre d'emploi gratuitement !

AGENDA

Salon e-Commerce
Du Mardi 23 septembre 2014 au Jeudi 25 septembre 2014

Fujitsu World Tour 2014
Le Jeudi 25 septembre 2014
09:00 - 17:30

Soirée-débat, le 30 septembre 2014, Paris
Le Mardi 30 septembre 2014
19:00 - 00:00

DCD Converged
Le Lundi 06 octobre 2014

IP EXPO Europe
Du Mercredi 08 octobre 2014 au Jeudi 09 octobre 2014

Voir tous les événements

SONDAGE EXPRESS

Pour la virtualisation, vous êtes plutôt...

- VMware
- Hyper-V
- KVM
- Xen

Votez
Voir les résultats

SILICON TV

THÉMATIQUES IT

4g
Byod
Big Data
Business Intelligence
Cloud
Mobilité
Open Source
Processeurs
Programmation
Stockage
Sécurité
Très Haut Débit

RECHERCHER UNE ENTREPRISE

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0 1 2 3 4 5 6 7 8 9

Vous pouvez utiliser ces balises et attributs HTML : <a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <i> <q cite=""> <strike>

Laisser un commentaire

Categories

Accueil
Composants
Telecoms
Infrastructure
Solutions
Workspace
Cyberpouvoirs
Cloud
Sécurité
Mobilité
Open-Source

Site

Contactez la rédaction
Contactez la régie
Contactez la technique
Proposition de partenariat
Charte de confiance - Mentions Légales
Conditions Générales d'Utilisation
Annoncer sur Silicon.fr
Inscription à la Newsletter
Votre compte
Plan du site
Test de bande passante
Quelle est mon adresse IP ?
Test Couverture 4G et spots Wifi

NetMediaEurope France

Livres Blancs Informatiques
Télécharger
Silicon
SiliconDSI
The Inquirer
ChannelBiz
Gizmodo
Emplois, jobs Informatique

NetMediaEurope

France
Royaume-Uni
Espagne
Allemagne
Italie
Portugal
Brésil

NetMediaEurope © Copyright 2014 Agence Presse Magazine. Tous droits réservés. A propos de NetMediaEurope